UNITED STATES PATENT AND TRADEMARK OFFICE
DOCUMENT CLASSIFICATION BARCODE SHEET

000

CATEGORY:

# CLEARED

ADDRESS
CONTACT IF FOUND:

| | |
|---|---|
| FORM-PTO-1390 (Rev. 12-29-99) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE | ATTORNEY'S DOCKET NUMBER<br>032326-105 |
| **TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371** | U S APPLICATION NO (If known, see 37 C F R 1 5)<br>Unassigned 19432 |

| | | |
|---|---|---|
| INTERNATIONAL APPLICATION NO.<br>PCT/FR98/01226 | INTERNATIONAL FILING DATE<br>12 June 1999 | PRIORITY DATE CLAIMED<br>12 June 1999 |

TITLE OF INVENTION
METHOD FOR VERIFYING THE EXECUTION OF A SOFTWARE PRODUCT

APPLICANT(S) FOR DO/EO/US
Louis GREGOIRE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

**Items 11. to 16. below concern other document(s) or information included:**

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☒ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

| U.S. APPLICATION NO. (If known,/ see 37 C.F.R. 1.50) | INTERNATIONAL APPLICATION NO | ATTORNEY'S DOCKET NUMBER |
|---|---|---|
| Unassigned 09/719432 | PCT/FR98/01226 | 032326-105 |

| | CALCULATIONS | PTO USE ONLY |
|---|---|---|
| 17. ☒ The following fees are submitted: | | |
| **Basic National Fee (37 CFR 1.492(a)(1)-(5)):** | | |
| Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO .......... $1,000.00 (960) | | |
| International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO .......... $860.00 (970) | | |
| International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ............ $710.00 (958) | | |
| International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) ............. $690.00 (956) | | |
| International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) ................. $100.00 (962) | | |
| **ENTER APPROPRIATE BASIC FEE AMOUNT =** | $ 860.00 | |
| Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 □ 30 □ months from the earliest claimed priority date (37 CFR 1.492(e)). | $ -0- | |

| Claims | Number Filed | Number Extra | Rate | | |
|---|---|---|---|---|---|
| Total Claims | 9 -20 = | -0- | X$18.00 (966) | $ -0- | |
| Independent Claims | 2-3 = | -0- | X$80.00 (964) | $ -0- | |
| Multiple dependent claim(s) (if applicable) | | | +$270.00 (968) | $ -0- | |

| | | |
|---|---|---|
| **TOTAL OF ABOVE CALCULATIONS =** | $ 860.00 | |
| Reduction for 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28). | $ -0- | - |
| **SUBTOTAL =** | $ 860.00 | |
| Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 □ 30 □ months from the earliest claimed priority date (37 CFR 1.492(f)). + | $ -0- | |
| **TOTAL NATIONAL FEE =** | $ 860.00 | |
| Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property + | $ -0- | |
| **TOTAL FEES ENCLOSED =** | $ 860.00 | |
| | **Amount to be: refunded** | $ |
| | **charged** | $ |

a. □ A check in the amount of $_______ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 02-4800 in the amount of $ 860.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

**NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.**

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

(Reg No 33096)
SIGNATURE

for James A. LaBarre
NAME

28,632
REGISTRATION NUMBER

Patent
Attorney's Docket No. 032326-105

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| In re Patent Application of | ) | |
| | ) | |
| Louis GREGOIRE | ) | Group Art Unit: Unassigned |
| | ) | |
| Application No.: Unassigned | ) | Examiner: Unassigned |
| | ) | |
| Filed: December 12, 2000 | ) | |
| | ) | |
| For: METHOD FOR VERIFYING THE EXECUTION OF A SOFTWARE PRODUCT | ) | |

## PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

**IN THE SPECIFICATION**:

Page 1, immediately following the title, insert the following:

--This disclosure is based upon, and claims priority from International Application No. PCT/FR98/01226, filed June 12, 1999, the contents of which are incorporated herein by reference.

**Background of the Invention**--;

Page 2, between lines 19 and 20, insert the following heading:

--**Summary of the Invention** --.

Add the following Abstract:

--The present invention relates to a method for verifying the execution of a computer program, comprising the following steps: 1) a program is split up into at least two parts, one public and one secret, whereby the public part is executed on a first processing means and the second part is executed on a second secure processing means; 2) the public part is placed in a memory pertaining to the first processing means; 3) the secret part is placed on a secure support pertaining to the second processing means in order to be connected to the first processing means; 4) the following operations are performed so that the program can be executed by the first processing means: a) the second processing means is connected to the first and parameters and variables that are a function of external signals triggered by a user are transmitted from the first processing means to the second, b) at least one part of the program is executed by the second processing means, implementing a certain number of received parameters/variables, c) the results of the execution as described in b) are transmitted from the second processing means to the first, d) a certain number of said results are used in the execution performed by the first means. The invention is characterized in that the second means is a portable and detachable auxiliary support which is provided with a chip.--

**IN THE CLAIMS**:

Kindly amend the following claims.

4. (Amended) Process according to [one of claims 1-3] claim 1, wherein the second processing means is a card having a microprocessor.

5. (Amended) Processing according to [one of claims 1-3] claim 1, wherein the second processing means is in a hardwired form on a memory card.

6. (Amended) Processing according to [any one of the preceding claims] claim 1, wherein the first processing means is a central processing unit of a computer.

7. (Amended) Process according to [any one of the preceding claims] claim 6, wherein the central processing unit is connected to a network, particularly of the Internet type, on which at least the public part of the program is available on demand.

8. (Amended) Processing according to [claims 2-7] claim 2, wherein a secure distribution is effected of utilization rights of the said program to a medium of a user via a server.

## REMARKS

Entry of the foregoing amendments is respectfully requested. These amendments are intended to further clarify the language of the claims and specification, as well as eliminate multiple dependencies.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: (Reg No 33096)
for James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: December 12, 2000

# PROCESS OF CONTROLLING A SOFTWARE PRODUCT

The present invention relates to the field of the protection of software products against piracy. It has as its object a process of controlling the execution of a software product.

A software product is understood to mean any program and/or data intended to be processed or executed by a central processing unit, particularly the microcomputer of a personal computer (PC). Software products can be recorded on any medium such as a diskette, hard disk, CD-ROM compact optical disk, or stored on any medium such as a ROM or EPROM type memory.

Computer programs or software products, particularly for a PC, are more and more copied and used without authorization. This is accentuated by the possibility of disseminating the copy on a large scale over networks of servers or to copy it by a mass production of CD-ROMs on which the software is recorded. Simple illegal copies which can be produced on a hard disk or on microcomputer diskettes within the same company are also known.

Among the solutions for preventing illegal use of software products, a system is known for controlling the distribution of computer programs. The program is recorded on its medium in a coded form, and it is then decoded before loading on the computer by the authorized user. For this purpose, the authorized user has means permitting decoding. This process has the advantage of preventing the copying of the medium containing the program, but it has the disadvantage of not preventing the copying of the program from the PC.

A process for controlling the execution of the program is likewise known. It consists of putting into effect a procedure which permits the verification of the presence of a secure device connected to the serial port of the PC, in particular, or to a printer port, this device proving by its presence that the user is authorized to use the program. The presence and authenticity of the device is verified during the execution of the program, continuing the execution of the program being dependent on the verification. This process has the disadvantage that it can be bypassed by skipping the instructions corresponding to this verification.

A process for controlling the use of a microcomputer by an authorized person, and thus indirectly of any program contained within it, is likewise known. It uses a chip card with a microcircuit, commonly known as a "smart card". In this process, a PC is connected via a suitable interface to the smart card, contains a secret authorization code. The authorized user has to key in the access code, which is compared with that stored in the smart card. If the codes correspond, access to the computer or to data or to a computer program is authorized.

This process has the disadvantage of not being able to directly protect the medium before it is loaded into the computer. The medium can therefore be copied.

In the following description, there is understood by "smart card", any accessory type of chip medium which is detachable and portable, and which comprises at least one security module containing a microprocessor and a memory space suitable for containing secret data such as a secret key, as well as secret programs. In particular, a module is concerned which can be inserted into an input/output port of a computer; preferably, it is a card of standardized form, a chip card, or a mini chip card.

The present invention has as its object to provide a solution to the problem of piracy which is more effective than the present solutions.

The solution provided by the invention likewise relates to the field of control of the execution of a computer program. Execution is controlled because it is solely permitted to persons who have purchased a right of utilization. This right is brought into effect by a secure means or accessory, particularly a smart card according to an example of the invention. By this means, any copying or diffusion of the program is deterred.

For this purpose, the invention firstly has as its object a process of control of the execution of a computer program. According to a first mode, it comprises the following steps, consisting of:

(1) Splitting a program into at least two parts, respectively public and secret, the public part being suitable for execution on a first processing means, and the secret part being suitable for execution on a secure, second processing means.

(2) Placing the public part in a memory of the first processing means.

(3) Placing the secret part on a secure medium of the second processing means intended to be connected to the first processing means.

(4) Carrying out the following operations for the execution of the program by the first processing means:

(a) connecting the second processing means to the first, and transmission, from the first processing means to the second, of parameters/variables which are functions of external signals initiated by a user,

(b) execution of at least a portion of the program by the second processing means, putting into effect a certain number of the said received parameters/variables,

(c) transmission of the results of the execution of the preceding paragraph (b) from the second processing means to the first,

(d) using a certain number of the said results in the execution effected by the first means.

It is characterized in that the second means is a portable and detachable accessory chip medium.

According to another embodiment, the process comprises the following steps consisting of:

(1) Splitting a program into at least two parts, respectively public and secret, the public part being suitable for execution on a first processing means, and the secret part being suitable for execution on a secure, second processing means.

(2) Encoding at least a secret part and placing it with the public part on the same medium, the latter being intended to be connected to the first processing means.

(3) Placing a corresponding decoding function in the second processing means.

(4) Carrying out the following operations for the execution of the program:

(a) connecting the second processing means to the first, and transmission, from the first processing means to the second, of all or a portion of the coded secret part,

(b) decoding the said coded secret part received by the second, secure processing means by making use of the said decoding function, and storing the decoded secret part in secure memory.

(c) transmission from the first processing means to the second of parameters/variables which are functions of external signals,

(d) execution of at least a secret portion by the second, secure processing means, using a certain number of the said received parameters/variables,

(e) transmission of the results of the execution of the preceding paragraph (d) from the second processing means to the first,

(f) using a certain number of the said results in the execution effected by the first means.

It is characterized in that the second means is a portable and detachable accessory chip medium.

According to a characteristic of implementation of the second variant, in the operation (a) a portion of the coded program is transmitted to the extent needed and/or as a function of the capacity of the secure, second processing means.

Due to this characteristic, a coded program can be executed which has a size greater than the memory capacity of the second processing means. This makes it possible to have recourse to easily manipulated, discrete portable media of the type with a chip, which are generally excluded as the second processing means because of their small capacity.

The invention will be better understood on reading the description of the two modes of embodiment of the process in connection with an example of a computer program.

The program taken as an example is a word processing program.

To put the process into effect, it is necessary to split the word processing program into at least two parts, respectively public and secret. The public part is capable of being executed on a first processing means, while the secret part is capable of being executed on a second, secure processing means. They can thus appropriately undergo a compilation which is distinct for each.

The first part, termed public, is executable on a microcomputer (PC) operating system, taken as the first processing means in the example.

The second part, termed secret, is executable on a secure circuit of a chip card, taken as the second processing means in the example. The secure circuit comprises an 8-bit processor, a ROM permanent memory containing the operating system of the card, and a non-volatile EEPROM type memory and a RAM type volatile working memory. The circuit can be, for example, the circuit of a smart card.

During the storage of the word processing program on a medium intended to be distributed commercially, the program is distributed on distinct storage or recording media. For this, in the example, the public part is disposed on an optical disk (CD-ROM), while the secret part is disposed in the EEPROM memory of the chip card. As the physical medium for the program, in this case, two elements are thus necessary: the optical disk and an associated chip card. In the example, the function of calculating the cursor position on the screen of a PC has been chosen to constitute the secret part. This function is lacking on the optical disk and is present solely on the chip card.

For the execution of the program, the PC is connected to the chip card by an interface so as to permit bidirectional communication between them. The public program of the optical disk is loaded into the PC by reading the optical disk. The chip card can for example be connected to the PC via a chip card reader which is itself connected to an input/output port of the PC.

In the course of execution according to the invention, the following operations or steps are effected.

Parameters/variables which are functions of external signals are transmitted from the first processing means to the second.

In a general manner, "external signals" means information or events which can be different for each utilization of the program. The security of the system is even better ensured when the set of information communicated to the card differs for each utilization. It is likewise even better ensured when the program on the chip card is complex because it comprises, for example, very numerous possible outputs and because there is a sophisticated relationship between the inputs and the outputs.

In the sense of the present invention, the actions initiated by the user via a mouse, keyboard or other input peripheral can for example constitute external signals.

In the example, it is the central processing unit of the PC which transmits to the card, via the interface, the data which correspond to keys of the keyboard actuated by the user. The central processing unit carries out this transmission by executing the public program and the functions of the operating system. For this purpose, the public program contains the instructions necessary for this transmission.

According to a following step of the process, at least a portion of the program is executed by the second, secure processing means, making use of a certain number of the said received parameters/variables. This implies that the output of the execution of this part of the program will strongly depend on the value or nature of the parameters/variables which are made use of or which are taken into account by the second processing means for the execution of the secret program.

In the example, when the user strikes the keys of the keyboard, the card then executes the calculation of the cursor position in a line of text on the screen and sends the result, in this case the value of this position, back to the PC, according to another step of the process.

Then, according to the process, the above results can be used as they are, or preferably a certain number of the above results can be taken into account or used in the execution effected by the first processing means. In the example, the central processing unit of the PC executes the public part of the program to display the position of the cursor on the screen.

It will be seen that the user cannot utilize the cursor function of word processing in the absence of the card. Any illegal copying of the word processing software is deterred by this means, since the software is unusable without the card. It will be understood that, due to the invention, the above deterrence will be more effective, the more the secret part corresponds to an essential part of the program.

Another mode of embodiment of the process of the invention will now be described.

The system required for the implementation of the process is identical to that described hereinabove, with the following differences.

The secret part is disposed in encoded form on the optical disk with the public part, instead of being disposed in the chip card.

The ROM memory of the chip card contains, besides the operating system, a function for decoding and for loading the decoded program into its RAM memory.

During the execution of the program according to the invention, the following operations or steps are carried out.

All or a portion of the encoded program is transmitted from the first processing means to the second.

In the example, it is the function of calculating the cursor position which is encoded. This is transmitted encoded by the word processing program to the chip card, for example on starting the program. It can likewise be transmitted only at the instant when it becomes necessary. For this purpose, the word processing program likewise includes information permitting the position to be localized, particularly its address or its filename.

According to the process, the said encoded secret part received by the second, secure processing means is decoded by implementing the said decoding function, and the decoded secret part is stored in secure memory.

In the example, the chip card decodes the function of calculating the cursor position by implementing its decoding function, and stores the function concerned in an executable form.

It will be seen in this example that the process implements a system comprising a smart card which is capable of loading all or a portion of the coded program, decoding with a secret key from the software publisher, receiving calls from the first means and transmitting them for the executable program which has been loaded beforehand, and returning the results to the first processing means.

The public executable program includes supplementary instructions for transmitting portions of secret program to the card, via the input/output functions of the operating system of the card or possibly via those of the operating system of the PC, and instructions for calls to functions loaded on the card.

By extension of the possible applications of the process of the invention, the decoder of the second processing means can be in a hardwired form on a memory card, in order to reduce the cost of the accessory.

As for the first processing means, it is generally a central processing unit of a personal computer.

Advantageously, before loading the public part onto the first processing means such as a PC, the public part can be disposed on a server or a database to which the central processing unit of the first means can be connected. The public part of a program or software product can likewise be disposed on a network, particularly of the Internet type, to which the first processing means can be connected as the user wishes.

Thus, for a potential purchaser of a software product, it is sufficient to search the software accessible on the network such as the Internet, and to load it into the memory of his PC. In parallel, the purchaser can receive the card containing the secret part, in particular by mail.

Although the software is available to everyone on the Internet network, it can only be used if the user has the accessory, particularly in the form of a card having a microprocessor.

Thus, by this means, the invention permits the software publisher to free himself from the copying of these last on a physical medium such as a diskette. The invention likewise dispenses with the physical distribution of the software.

Accompanying the executable software placed on the Internet, it is possible to add data such as the contents of a user's manual for the software.

Process of Distribution of Rights:

The invention described hereinabove enables the distribution of the software itself to be separated from the distribution of the rights of utilization. The software can be freely copied by users and/or placed at their disposal on a local or distant server, without restriction of access. This is the case for the public part as well as for the secret part in the case that this has been encoded, as described in the second variant. On the other hand, the distribution of the rights has to be secured to ensure that the use of the software is only granted after payment.

In the first variant described hereinabove, the rights are realized in the form of the secret part of the program stored on the card. Indeed, only those who possess a card with this secret program can use the software. In the second variant, the rights are realized by a secret cryptographic key which enables the second processing means (security module) to decode the secret code which is transmitted to it.

In the two variants which have been described, the rights (secret program or secret key) are loaded into the security module before its distribution. It is likewise possible to distribute these elements to an already distributed card, by means such as a public network (such as the Internet) to which the PC with the user's card is connected, or by the insertion of the card in a point of sale device at a software retailer's. A third means consists of establishing communication between a remote rights distribution server and the utilizing PC via the telephone network by means of a modem. The remote distribution of rights makes it possible to download new rights into a card which already contains rights, for example, for a new item of software whose public program is freely accessible elsewhere, either through a network or from a friend's copy, or for example because the initial CD-ROM (compact optical disk) contains several software products but the user has only purchased the rights to one of them. It also enables the distribution of the cards to be separated from the distribution of rights, which for example permits several software publishers to utilize the protection ensured by the same card. The card which has become neutral can in this case be purchased by an end user from the microcomputer retailer.

To effect the distribution of the key or of the secret program in a secure manner, a first variant of the process is described hereinbelow. It is supposed that the starting card does not contain any rights.

(1) The issuer of the card includes on it, before distribution, and in addition to the elements described hereinabove in the two variants of the invention, a decoding means and a secret key, intended to decode the rights (which in one case

are themselves represented by a key). Furthermore, he includes there a unique number (different for each card) which is termed the "identity" of the card.

(2) The issuer of the card places at the disposal of software publisher(s) a decoding means for the rights and its encoding key, for the particular programs of this publisher or these publishers. The encoding key is in this case identical to the decoding key contained in the user's card.

(3) During the purchase of rights, the purchaser places his card in communication with the rights distribution server, which itself is connected to the rights coding means. This can be effected, for example, from the user's home, the office, or at a point of sale for software, via any data communication means such as the Internet network, a modem connection, or the use of the communication means of the networks of mobile telephones equipped with a card reader.

(4) After verification of payment by some means, (not described here but which can make use of a manual transaction with cash or a check to the storekeeper, or an automatic transaction with the same or another remote server, making use of specific payment functions of the operating system of the same or another card), the card sends to the server a request for loading the rights. This request includes an identification of the software product requested, as well as the identity of the card.

(5) The server combines the identity of the card with the rights coding key, for example, by a logical XOR operation, the result being a number of bits suitable for use as the encoding key. This process is termed diversification of the key. The server uses this diversified key to encode the requested rights. It makes it possible to guarantee that the thus encoded rights will only be usable by the card which has requested them, and in particular cannot be loaded onto other cards.

(6) The server sends the thus encoded rights to the purchaser's card.

(7) The purchaser's card effects the same operation combining encoding key and identity to calculate the decoding key. It uses this to decode the rights, and

stores them in its non-volatile memory. It then has the means to execute the secret part of the program which has been purchased.

CLAIMS

1. Process of controlling the execution of a computer program, comprising the following steps consisting of:

(1) Splitting a program into at least two parts, respectively public and secret, the public part being suitable for execution on a first processing means, and the secret part being suitable for execution on a secure, second processing means.

(2) Placing the public part in a memory of the first processing means.

(3) Placing the secret part on a secure medium of the second processing means intended to be connected to the first processing means.

(4) Carrying out the following operations for the execution of the program by the first processing means:

(a) connecting the second processing means to the first, and transmission, from the first processing means to the second, of parameters/variables which are functions of external signals initiated by a user,

(b) execution of at least a portion of the program by the second processing means, putting into effect a certain number of the said received parameters/variables,

(c) transmission of the results of the execution of the preceding paragraph (b) from the second processing means to the first,

(d) using a certain number of the said results in the execution effected by the first means, **wherein** the second means is a portable and detachable accessory chip medium.

2. Process of controlling the execution of a computer program, comprising the following steps consisting of:

(1) Splitting a program into at least two parts, respectively public and secret, the public part being suitable for execution on a first processing means, and the secret part being suitable for execution on a secure, second processing means.

(2) Encoding at least a secret part and placing it with the public part on the same medium, the latter being intended to be connected to the first processing means.

(3) Placing a corresponding decoding function on the second processing means.

(4) Carrying out the following operations for the execution of the program:

(a) connecting the second processing means to the first, and transmission, from the first processing means to the second, of all or a portion of the encoded secret part,

(b) decoding the said encoded secret part received by the second, secure processing means by making use of the said decoding function, and storing the decoded secret part in secure memory,

(c) transmission from the first processing means to the second of parameters/variables which are functions of external signals,

(d) execution of at least a secret portion by the second, secure processing means, using a certain number of the said received parameters/variables,

(e) transmission of the results of the execution of the preceding paragraph (d) from the second processing means to the first,

(f) using a certain number of the said results in the execution effected by the first means;

**wherein** the second means is a portable and detachable accessory chip medium.

3. Process according to claim 2, wherein, in the operation (a), a portion of the encoded program is transmitted to the extent needed and/or as a function of the capacity of the second, secure processing means.

4. Process according to one of claims 1-3, wherein the second processing means is a card having a microprocessor.

5. Process according to one of claims 1-3, wherein the second processing means is in a hardwired form on a memory card.

6. Process according to any one of the preceding claims, wherein the first processing means is a central processing unit of a computer.

7. Process according to any one of the preceding claims, wherein the central processing unit is connected to a network, particularly of the Internet type, on which at least the public part of the program is available on demand.

8. Process according to claims 2-7, wherein a secure distribution is effected of utilization rights of the said program to a medium of a user via a server.

9. Process according to claim 8, characterized in that the support sends to a server a request for loading rights, containing the identity of the program and an identity of the medium, the said server combines an identity of the requester's medium with a rights encoding key, the result being a number of bits suitable for use as a diversified encoding key, the server uses this diversified key to encode the requested rights, and sends the thus encoded rights to the requester's medium.

**COMBINEDDECLARATIONFORPATENTAPPLICATIONANDPOWEROFATTORNEY**
**(IncludesReferencetoProvisionalandPCTInternationalApplications)**

Attorney'sDocketNo.

Asabelownamedinventor,Iherebydeclarethat:
Myresidence,postofficeaddressandcitizenshipareasstatedbelownexttomyname,
IbelieveIamtheoriginal,firstandsoleinventor(ifonlyonenameislistedbelow)oranoriginal,firstandjointinventor(ifpluralnamesarelistedbelow)ofthesubjectmatterwhichisclaimedandforwhichapatentissoughtontheinvention entitled:

METHOD FOR VERIFYING THE EXECUTION OF A SOFTWARE PRODUCT.

thespecificationofwhich(checkonlyoneitembelow)

- isattachedhereto
- wasfiledasUnitedStatesapplication
  Number ________
  on ________
  andwasamended
  on ________ (ifapplicable)
- wasfiledasPCTinternationalapplication
  Number PCT/FR 98/01226
  on June 12th 1998
  andwasamended
  on ________ (ifapplicable)

IherebystatethatIhavereviewedandunderstandthecontentsoftheabove-identifiedspecification,includingtheclaims,as amendedbyanyamendmentreferredtoabove

IacknowledgethedutytodisclosetotheOfficeallinformationknowntometobematerialtopatentabilityasdefinedinTitle 37,CodeofFederalRegulations,§1.56

IherebyclaimforeignprioritybenefitsunderTitle35,UnitedStatesCode,§119(a)-(e)ofanyforeignapplication(s)forpatent orinventor'scertificateorofanyPCTinternationalapplication(s)designatingatleastonecountryotherthantheUnitedStates ofAmericalistedbelowandhavealsoidentifiedbelowanyforeignapplication(s)forpatentorinventor'scertificateoranyPCT internationalapplication(s)designatingatleastonecountryotherthantheUnitedStatesofAmericafiledbymeonthesame subjectmatterhavingafilingdatebeforethatoftheapplication(s)ofwhichpriorityisclaimed

PRIORFOREIGN/PCTAPPLICATION(S)ANDANYPRIORITYCLAIMSUNDER35U.S C.§119:

| COUNTRY<br>(ifPCT,indicate"PCT") | APPLICATIONNUMBER | DATEOFFILING<br>(day,month,year) | PRIORITYCLAIMED<br>UNDER35U S.C §119 |
|---|---|---|---|
| FRANCE . | 97 05328 | 16.04.1997. | _Yes _No |
| PCT . | WO 99/66387 | 23.12.1999 | _Yes _No |
| | | | _Yes _No |
| | | | _Yes _No |
| | | | _Yes _No |

IherebyclaimthebenefitunderTitle35,UnitedStatesCode§119(e)ofanyUnitedStatesprovisionalapplication(s)listed below.

________ (ApplicationNumber) ________ (FilingDate)

________ (ApplicationNumber) ________ (FilingDate)

| COMBINEDDECLARATIONFORPATENTAPPLICATIONANDPOWEROFATTORNEY(CONT'D)<br>(IncludesReferencetoProvisionalandPCTInternationalApplications) | Attorney'sDocketNo. |
|---|---|

IherebyclaimthebenefitunderTitle35,UnitedStatesCode,§120ofanyUnitedStatesapplications(s)orPCTinternational application(s)designatingtheUnitedStatesofAmericathatis/arelistedbelowand,insofarasthesubjectmatterofeachofthe claimsofthisapplicationisnotdisclosedinthat/thosepriorapplication(s)inthemannerprovidedbythefirstparagraphof Title35,UnitedStatesCode,§112,IacknowledgethedutytodisclosetotheOfficeallinformationknowntometobematerial tothepatentabilityasdefinedinTitle37,CodeofFederalRegulations§1 56,whichbecameavailablebetweenthefilingdate ofthepriorapplication(s)andthenationalorPCTinternationalfilingdateofthisapplication:

PRIORU S.APPLICATIONSORPCTINTERNATIONALAPPLICATIONSDESIGNATINGTHEU S.FORBENEFITUNDER35U S.C. §120:

| U.S.APPLICATIONS | | | STATUS *(checkone)* | | |
|---|---|---|---|---|---|
| U S APPLICATIONNUMBER | U S FILINGDATE | | PATENTED | PENDING | ABANDONED |
| | | | | | |
| | | | | | |
| | | | | | |
| PCTAPPLICATIONSDESIGNATINGTHEU.S. | | | | | |
| PCTAPPLICATIONNO | PCTFILINGDATE | U S APPLICATIONNUMBERS ASSIGNED*(ifany)* | | | |
| | | | | | |
| | | | | | |
| | | | | | |

09719432.021601

IherebyappointthefollowingattorneysandagentS(s)toprosecutesaidapplicationandtotransactallbusinessinthePatentand TrademarkOfficeconnectedtherewithandtofile,prosecuteandtotransactallbusinessinconnectionwithinternational applicationsdirectedtosaidinvention

| | | | | | |
|---|---|---|---|---|---|
| WilliamL Mathis | 17,337 | R DannyHuntington | 27,903 | GeraldF Swiss | 30,113 |
| RobertS Swecker | 19 885 | ErichH Weisblatt | 30,505 | MichaelJ Ure | 33,089 |
| PlatonN Mandros | 22,124 | JamesW Peterson | 26,057 | CharlesF WielandIII | 33,096 |
| BentonS Duffett,Jr | 22,030 | TeresaStanekRea | 30,427 | BruceT Wieder | 33,815 |
| NormanH Stepno | 22,716 | RobertE Krebs | 25,885 | ToddR Walters | 34,040 |
| RonaldL Grudziecki | 24,970 | WilliamC Rowland | 30,888 | RonniS Jillions | 31,979 |
| FrederickG Michaud,Jr | 26,003 | T GeneDillahunty | 25,423 | HaroldR BrownIII | 36,341 |
| AlanE Kopecki | 25,813 | PatrickC Keane | 32,858 | AllenR Baum | 36,086 |
| RegisE Slutter | 26,999 | BruceJ Boggs,Jr | 32,344 | StevenM duBois | 35,023 |
| SamuelC Miller,III | 27,360 | WilliamH Benz | 25 952 | BrianP O'Shaughnessy | 32 747 |
| RobertG Mukai | 28,531 | PeterK Skiff | 31,917 | KennethB Leffler | 36,075 |
| GeorgeA Hovanec,Jr | 28 223 | RichardJ McGrath | 29,195 | FredW Hathaway | 32,236 |
| JamesA LaBarre | 28 632 | MatthewL Schneider | 32,814 | | |
| E.JosephGess | 28,510 | MichaelG Savage | 32,596 | | |

21839

and: ______________________________

Addressallcorrespondenceto.

21839

JamesA LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L P
P O Box1404
Alexandria,Virginia22313-1404

AddressalltelephonecallstoJamesA LaBarre at(703)836-6620.

Iherebydeclarethatallstatementsmadehereinofmyownknowledgearetrueandthatallstatementsmadeoninformation andbeliefarebelievedtobetrue;andfurtherthatthesestatementsweremadewiththeknowledgethatwillfulfalsestatements andthelikesomadearepunishablebyfineorimprisonment,orboth,underSection1001ofTitle18oftheUnitedStates Codeandthatsuchwillfulfalsestatementsmayjeopardizethevalidityoftheapplicationoranypatentissuedthereon

**COMBINEDDECLARATIONFORPATENTAPPLICATIONANDPOWEROFATTORNEY(CONT'D)**
**(IncludesReferencetoProvisionalandPCTInternationalApplications)**

Attorney'sDocketNo.

100

FULLNAMEOFSOLEORFIRSTINVENTOR
Louis GREGOIRE.

SIGNATURE

DATE
Nov 13th 2000

RESIDENCE
31 Allée des Tamaris

CITIZENSHIP
FRANCE

POSTOFFICEADDRESS
31 Allée des Tamaris Les Terrasses de Cassis 13260 CASSIS

FULLNAMEOFSECONDJOINTINVENTOR,IFANY

SIGNATURE

DATE

RESIDENCE

CITIZENSHIP

POSTOFFICEADDRESS

FULLNAMEOFTHIRDJOINTINVENTOR,IFANY

SIGNATURE

DATE

RESIDENCE

CITIZENSHIP

POSTOFFICEADDRESS

FULLNAMEOFFOURTHJOINTINVENTOR,IFANY

SIGNATURE

DATE

RESIDENCE

CITIZENSHIP

POSTOFFICEADDRESS

FULLNAMEOFFIFTHJOINTINVENTOR,IFANY

SIGNATURE

DATE

RESIDENCE

CITIZENSHIP

POSTOFFICEADDRESS

FULLNAMEOFSIXTHJOINTINVENTOR,IFANY

SIGNATURE

DATE

RESIDENCE

CITIZENSHIP

POSTOFFICEADDRESS

FULLNAMEOFSEVENTHJOINTINVENTOR,IFANY

SIGNATURE

DATE

RESIDENCE

CITIZENSHIP

POSTOFFICEADDRESS

FULLNAMEOFEIGHTHJOINTINVENTOR,IFANY

SIGNATURE

DATE

RESIDENCE

CITIZENSHIP

POSTOFFICEADDRESS

# GENERAL POWER OF ATTORNEY

Gemplus, S.A., through its undersigned representative, hereby appoints James A. LaBarre, Registration No. 28,632, and Mark. R. Kresloff, Registration No. 42,766, as its attorneys, with full power to prosecute, transact all business in the U.S. Patent and Trademark Office, and appoint associate attorneys in connection with each and every patent and patent application in which Gemplus, S.A. has an ownership interest. Please direct all correspondence as follows:

James A. LaBarre  
BURNS, DOANE, SWECKER & MATHIS, L.L.P  
Post Office Box 1404  
Alexandria, Virginia 22313-1404  
(703) 836-6620

The undersigned (whose title appears below) is empowered to sign this document on behalf of Gemplus, S.A.

Date: June 8, 2000

Signature: B  
Bernard Nonnenmacher

Title: Director of Intellectual Property